PR 1803079

McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Dominic A. Paluzzi
Direct Dial: 248.220.1356
dpaluzzi@mcdonaldhopkins.com

January 19, 2018

State of Connecticut
Office of the Attorney General
55 Elm St.
Hartford, CT 06106

Re: Rogin Nassau LLC – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Rogin Nassau LLC ("Rogin Nassau"). I write to provide notification concerning an incident that may affect the security of personal information of one hundred seventy (170) Connecticut residents. Rogin Nassau's investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, Rogin Nassau does not waive any rights or defenses regarding the applicability of Connecticut law or personal jurisdiction.

On or about July 28, 2017, Rogin Nassau initially detected some suspicious emails being sent from a limited group of its employee email accounts. Upon learning of the issue, Rogin Nassau promptly changed the password to the affected email accounts and maintained heightened monitoring of the accounts to ensure that no other suspicious activity was taking place. In addition, Rogin Nassau simultaneously commenced an investigation of the incident and retained an independent computer forensic firm to analyze the extent of any compromise to the email accounts and the security of the emails and attachments contained within them.

Since completing the investigation and manual document review, which concluded on or about November 3, 2017, Rogin Nassau concluded that an unauthorized third party accessed the email accounts at issue. The forensic investigation could not definitively conclude what information within the account, if any, was actually accessed, viewed, downloaded or otherwise acquired by the unauthorized user. The forensic firm also confirmed that this incident did not impact the security of any other email accounts, our networks or servers.

Further, based on the investigation conclusions, Rogin Nassau has devoted considerable time and effort to determine what information was contained in the affected email accounts. Rogin Nassau conducted a sophisticated review of each email and attachment contained within the compromised email accounts that was forensically identified as having contained personal information to ensure accuracy and confirm those potentially impacted. Rogin Nassau confirmed

that the compromised email accounts contained residents' name and Social Security number, and may have included driver's license number and/or bank account information.

To date, Rogin Nassau is not aware of any confirmed instances of identity fraud as a direct result of this incident. Nevertheless, Rogin Nassau wanted to make you (and the affected residents) aware of the incident and explain the steps Rogin Nassau is taking to help safeguard the residents against identity fraud. Rogin Nassau provided the Connecticut residents with written notice of this incident commencing on January 19, 2018, in substantially the same form as the letter attached hereto. Rogin Nassau is offering the residents a complimentary membership with a credit monitoring and identity theft protection service. Rogin Nassau has advised the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. Rogin Nassau has advised the residents about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. The residents also have been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Rogin Nassau takes its obligation to help protect personal information very seriously. Rogin Nassau is continually evaluating and modifying its practices to enhance the security and privacy of confidential information, and has taken steps to strengthen access controls and protocols to help prevent similar issues in the future.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,

Dominic A. Paluzzi

Encl.

ROGIN NASSAU LLC
Attorneys at Law
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

[redacted]

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

[redacted]

Dear [redacted]:

The privacy and security of your personal information is of the utmost importance to Rogin Nassau LLC. I am writing with important information about a recent incident potentially involving the security of some of your personal information that is maintained by Rogin Nassau. We want to provide you with information regarding the incident and explain the services we are making available to help safeguard you against identity fraud. We also are providing additional steps you can take to help protect your information.

What Happened?

On or about July 28, 2017, Rogin Nassau initially detected some suspicious emails being sent from a limited group of its employee email accounts. Upon learning of the issue, we promptly changed the password to the affected email accounts and maintained heightened monitoring of the accounts to ensure that no other suspicious activity was taking place. In addition, we simultaneously commenced an investigation of the incident and retained an independent computer forensic firm to analyze the extent of any compromise to the email accounts and the security of the emails and attachments contained within them.

Since completing our investigation and manual document review, which concluded on or about November 3, 2017, we concluded that an unauthorized third party accessed the email accounts at issue. The forensic investigation could not definitively conclude what information within the account, if any, was ***actually*** accessed, viewed, downloaded or otherwise acquired by the unauthorized user. The forensic firm also confirmed that this incident did not impact the security of any other email accounts, our networks or servers.

What We Are Doing.

Further, based on the investigation conclusions, we have devoted considerable time and effort to determine what information was contained in the affected email accounts. We conducted a sophisticated review of each email and attachment contained within the compromised email accounts that was forensically identified as having contained personal information to ensure accuracy and confirm those potentially impacted.

What Information Was Involved.

Because we value our relationship with you, we wanted to notify you of this incident since your personal information was contained within one of the compromised email accounts, which included your full name and Social Security number.

What You Can Do.

To date, we are not aware of any reports of identity fraud, theft, or improper use of information as a direct result of this incident. Out of an abundance of caution, however, we wanted to provide you with information regarding the incident and explain the services we are making available to help safeguard you against identity fraud.

To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorks^{SM} Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter. Also enclosed in this letter, you will find information about other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

For More Information.

Please know that we take this situation very seriously and regret any inconvenience or concern this incident may cause you. Maintaining the integrity of your personal information is of the utmost importance to us and we have taken steps to strengthen access controls and protocols to help prevent similar issues in the future.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9:00 a.m. to 5:00 p.m. Eastern Time.

Sincerely,

Rogin Nassau LLC

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks[SM] Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **March 22, 2018** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll [redacted]
3. PROVIDE the **Activation Code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted]. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at [redacted]
or call [redacted] to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [redacted].

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others. Alternatively, you may file the Fraud Alert online. Here is a link to the Experian fraud alert home page: https://www.experian.com/fraud/center.html

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-888-766-0008
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
https://www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/freeze/center.html

TransUnion Security Freeze (FVAD)
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
https://freeze.transunion.com/

Please note that there may be a charge associated with placing, temporarily lifting, or removing a security freeze with each of the above credit reporting companies. These fees vary by state, so please call or visit the credit reporting agencies' websites to find out the specific costs applicable to the State in which you currently reside.

If you decide to place a Security Freeze on your credit file, *in order to do so without paying a fee*, you will need to send a copy of a valid identity theft report or police report, by mail, to each credit reporting company to show that you are a victim of identity theft and are eligible for free security freeze services. If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and monitoring free credit reports for any unauthorized activity. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC and/or the Attorney General's office in your state. You can obtain information from these sources about the steps individuals can take to protect themselves from identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at https://www.identitytheft.gov/, by phone at 1-877-IDTHEFT (438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations.

For North Carolina Residents:
In addition to the FTC, you may obtain information about preventing identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: (919) 716-6400
Toll-free: (877) 566-7226
Fax: (919) 716-6750
Website: http://www.ncdoj.gov
Email: consumer@ncdoj.gov

Instances of known or suspected identity theft should also be reported to law enforcement.

For Oregon Residents:
In addition to the FTC, you may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached at:

Oregon Department of Justice
Attorney General's Office
1162 Court Street NE
Salem, OR 97301-4096
Telephone: 877-877-9392
Website: www.doj.state.or.us

6. Reporting Identity Fraud to the IRS.

If you believe you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended you do the following:

- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf.
- Call the IRS at (800) 908-4490, ext. 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm.
- Report the situation to your local police or law enforcement department.

Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection.

7. Reporting Identity Fraud to the Social Security Administration.

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount.

- The Social Security Administration has published Identity Theft and Your Social Security Number at: https://www.ssa.gov/pubs/EN-05-10064.pdf.